LaTeX Blockchain технологийг сонгуулийн санал хураалтад ашиглах нь

Горилогч

© *Э.Төгөлдөр*

Энэхүү бүтээл нь

"Системийн ажуулгүй байдал" -аар баклаврын зэрэг

горилсон бүтээлд тавигдах

шаардлагыг бүрэн хангасан болно

Мэдээллийн сүлжээ ажуулгүй байдал

Шинжлэх Ухаан Технологийн Их Сургууль

2017-10-18

Улаанбаатар хот

Гарчиг

Хүснэгтийн жагсаалт

Зургийн жагсаалт

Бүлэг 1

Удиртгал

1.1 Зорилго

Бүлэг 2

Онол

2.1 Блокчэйн технологи

2.1.1 Түүх

Анхандаа блокчэйн нь компьютерын шинжлэх ухаанд мэдээллийг хэрхэн зохион байгуулах болон дамжуулах талаарх нэр томьёо төдий байсан. Харин өнөөдөр блокчэйн нь компьютерын хөгжлийн "5 дахь хувьсал"хэмээн өргөмжлөгдөж байна.

Анхны криптографын шифрлэлтээр хамгаалагдсан блокуудын сүлжээг 1991 онд Стюарт Хабер(Stuart Haber) В. Скотт Сторнетта(W. Scott Scornetta) нар танилцуулсан. 1992 онд Баер, Хабер, Сторнетта нар блокчэйнд Merkle trees - г холбосноор нэг блокт хэд хэдэн мэдээллийг цуглуулах боломжтой болж ажлын чадамж нь нэмэгдсэн.

Анхны төвлөрсөн бус блокчэйний концепцыг 2008 онд Сатоши Накамото(Satoshi Nakamoto) гаргаж, дараа жил нь цахим мөнгөн тэмдэгт болох bitcoin - ны цөм хэсэгтэй холбож өгснөөр цахим гүйлгээ бүрд нийтийн данс(ledger) маягаар ашиглах боломжтой болгосон. Peer-to-peer сүлжээ болон төвлөрсөн бус цаг бүртгэлийн серверүүдээр блокчэйний мэдээллийн сан автоматаар зохицуулагдаж байдаг. Bitcoin - д блокчэйнийг ашигласан нь давхар төлөлт буюу цахим гүйлгээнд нэг тоон токен нэгээс илүү ашиглагдах асуудлыг итгэмжлэгдсэн зохион байгуулагчийн шаардлагагүйгээр шийдсэн анхны тоон мөнгөн тэмдэгт болсон.

Блок болон чэйн гэх үгүүд нь Сатоши Накамото - ийн 2008 оны 10-р сарын анхны эрдэм шинжилгээний нийтлэлд салангид бичигдэн хэрэглэгдсэн байсан бөгөөд олон нийтэд алдаршиж блокчэйн гэх нэг үг болтлоо 2016 оныг хүртэл блок чэйн гэх салангид үг байдлаар ашиглагдаж байсан.

2014 онд "Блокчэйн 2.0"нь төвлөрсөн бус өгөгдлийн сангийн блокчэйн програмуудыг илтгэсэн нэршил болж гарч ирсэн. Блокчэйн 2.0 технологи ашигласнаар цахим гүйлгээнд утга солилцоход мөнгө болон мэдээллийн арбитрын үүрэгтэй зуучлагчийн шаардлагагүй болгосон. Хоёрдугаар үеийн блокчэйн технологи хувь хэрэглэгчдийн цахим тодорхойлолт болон хувийн мэдээллийг хадгалах боломжтой болсон.

2016 онд Оросын холбооны сангийн аюулгүй байдлын төв Nxt Блокчэйн 2.0 платформд суурилсан автомат санал хураалтын системийн хэрэглээг судлах туршилтын төслийг зарласан. Хөгжмийн зах зээлийн төлөөлөл болсон байгууллагууд олноор блокчэйн технологи ашиглан оюуны өмчийн эрхийн шимтгэлийг цуцлуулах, зохиогчийн эрхийг удирдан хянах ажлыг дэлхий нийтээр хэрэгжүүлэх туршилтын загваруудыг туршсаар байна. IMB 2016 оны 7-р сард Сингапур улсад блокчэйний шинэчлэлт болон судалгааны төвөө нээсэн.

2017 оны эхээр Хаврард бизнес шүүмж (Harvard Business Review) сэтгүүлд блокчэйн бол өнөөгийн эдийн засгийн болон нийгмийн системд шинэ үндэслэл бий болгох чадамж бүхий суурь технологи юм гэсэн санал илэрхийлсэн нийтлэл бичжээ.

2.1.2 Блокчэйн гэж юу вэ

Блокчэйн гэдэг нь бие даасан хэрэглэгчдийн сүлжээ хооронд цахим мэдээллийн сан үүсгэх болон хуваалцах боломжтой болгох мэдээллийн зохион байгуулалт юм. Блокчэйн нь төвлөрсөн бус өгөгдлийн сангийн технологид шинэ шийдэл болж өгсөн. Энэ шинэчлэлт нь хуучин технологийг шинэ арга замтай холбосноор илүү сайжирч хөгжиж байна. Одоо блокчэйнийг бие даасан хэрэглэгчдийн нэгдэл мэдээллийн санг хадгалж, мэдээллийг хуваалцаж мөн удирдаж ажиллах төвлөрсөн бус өгөгдлийн сан гэж ойлгож болно. Олон төрлийн блокчэйн байдаг:

Нийтийн блокчэйн(Public blockchain) : (жишээ нь Bitcoin) нь давтагдашгүй токенуудаар ажиллах томоохон төвлөрсөн бус сүлжээ юм. Тэдгээр нь аль түвшний хэрэглэгчдэд нээлттэй ба тэдэнд дэмжлэг үзүүлэх нээлттэй эхийн кодууд байдаг.

Хувийн блокчэйн(Private blockchain) : нь ихэвчлэн жижиг хэмжээний сүлжээ байхаас гадна токен ашигладаггүй. Хэрэглэгчид нь нарийн хяналт дор үйл ажиллагаа явуулдаг. Энэ төрлийн блокчэйнүүд итгэмжлэгдсэн гишүүд болон нууцлагдсан дамжуулалттай холбоогоор баталгааждаг.

Зөвшөөрөгдсөн блокчэйн(Permissioned blockchain) : (жишээ нь Ripple) нь

нийтийн болон хувийн блокчэйнүүдийн хосолмол шинжтэй, хувийн блокчэйнтэй ижил хяналттай боловч хянагч нь сүлжээний хэрэглэгч дотроосоо байдаг. Нийтийн блокчэйнтэй ижлээр томоохон төвлөрсөн бус систем байх ба тэдгээр нь давтагдашгүй токен ашиглана. Код нь зарим нь нээлттэй эхийн, зарим нь нээлттэй эхийн бус байдаг.

Дээрх гурван төрлийн блокчэйнууд гурвуулаа криптограф ашиглан аль ч өгөгдсөн сүлжээнээс хэрэглэгч бүрийг төвлөрсөн хянагчийн шаардлагагүйгээр сүлжээнд хэрэгжиж буй дүрмүүдийг хэрэгжүүлэх, данс бүрийг хянах боломжийг олгодог. Төвлөрсөн хянагчийг өгөгдлийн сангийн бүтцээс халсан нь блокчэйн технологийн хамгийн ашигтай бөгөөд чухал шинж болсон юм.

Блокчэйн хэдий гүйлгээний байнгын бичилт болон түүхийг үүсгэж байдаг ч мөнхийн зүйл гэж байдаггүй. Гүйлгээний бичилтийн байнгын ажиллагаа нь сүлжээний тогтвортой байдлаас хамаардаг. Блокчэйний хувьд энэ нь том хэмжээний блокчэйний нэгдлийн гишүүн нэг бүр мэдээлэлд өөрчлөлт орсныг зөвшөөрөх болон зөвшөөрөхгүй байхыг шийдэж байж эцсийн өөрчлөлт хийгдэнэ гэсэн үг юм.

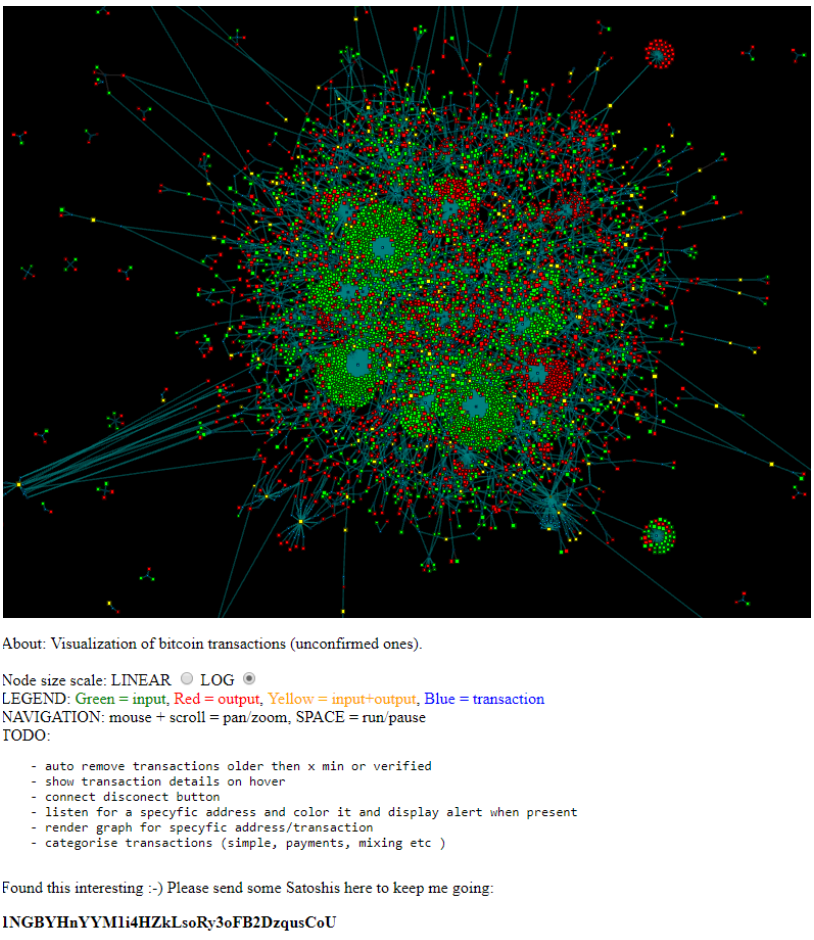
Мэдээлэл блокчэйнд нэгэнт бичигдсэн тохиолдолд үүнийг өөрчлөх эсвэл устгах нь бараг боломжгүй зүйл юм. Хэрэв хэн нэгэн блокчэйнд бичилт хийх буюу өөрөөр хэлбэл гүйлгээ хийх эсвэл дансны харилцаа хийхийг хүсвэл сүлжээн дэх батлах эрхтэй хэрэглэгчид тухайн захиалсан гүйлгээг баталгаажуулна. Үүнд л блокчэйний хамгийн төвөгтэй хэсэг оршдог учир нь блокчэйн бүр хэн хэрхэн ажиллах, хэн гүйлгээг баталгаажуулах зэргээр бие биеэсээ бага зэрэг өөр үүрэгтэй ажилладаг.

2.1.3 Блокчэйн юу хийдэг вэ

Блокчэйн нь ямар нэг мэдээллийн урсгалыг зохицуулагч төвлөрсөн удирдлагагүй peer-to-peer систем юм. Мэдээллийн бүрэн бүтэн, аюулгүй байдлыг хангахын зэрэгцээ төвлөрсөн хяналтыг халах нэг чухал арга нь бие даасан хэрэглэгчид бүхий том хэмжээний төвлөрсөн бус сүлжээтэй байх явдал юм. Ингэснээр тэдгээр компьютерууд тухайн сүлжээг нэгээс олон байршилд байршуулж байна гэсэн үг юм.

Блокчэйн төвлөрсөн бус байдалтай байгаа нь сүлжээний найдвартай байдлыг хангахаас гадна криптовалиутыг ашиглах боломжоор хангах зорилготой. Криптовалиут гэдэг нь дижитал токен бөгөөд зах зээлийн үнэлгээтэй, хувьцааны адилаар мөнгөн дэвсгэртээр арилжаалагддаг.

Криптовалиут нь блокчэйн бүрт бага зэрэг ялгаатай ажилладаг. Ерөнхийдөө техник



Зураг 2.1: Блокчэйн сүлжээний бүтэц. Бодит хугацааны хөдөлгөөнт загварыг http://dailyblockchain.github.io -с үзэж болно.

хангамжуудыг ажиллуулах програм хангамжууд урьдчилан бэлтгэгдсэн байдаг. Тэдгээр програм хангамжууд нь блокчэйний протокол юм. Бидний сайн мэдэх блокчэйн протоколуудад Bitcoin, Ethereum, Ripple, Hyperledger болон Faction зэрэг орно. Зангилаа хэрэглэгчийн техник хангамжийн бүрэлдэхүүн нь сүлжээн дэх мэдээллүүдийг баталгаажуулж байдаг.

2.1.4 Блокчэйн яагаад хэрэгтэй вэ

Блокчэйнийг өнөөдөр компьютерын ухаанд "тав дахь хувьсал"буюу интернетэд өмнө нь байгаагүй "итгэлцлийн түвшин"гэж нэрлэж байна. Энэ нь блокчэйн өнөөдөр дэлхий дахинд маш олон хүний анхаарлын төвд байх гол шалтгаан болж байна.

Блокчэйн цахим мэдээлэлд итгэлцэл үүсгэж байна. Мэдээлэл блокчэйнд нэгэнт би-

чигдсэн тохиолдолд үүнийг устгах эсвэл засварлах нь бараг л боломжгүй зүйл юм. Энэ боломж нь өмнө нь компьютерын сүлжээний орчинд огт байгаагүй зүйл юм.

Мэдээлэл дижитал хэлбэрт тогтвортой бөгөөд найдвартай байх боломжтой болсон тул өмнө нь гүйлгээний ажлыг зөвхөн онлайн бус горимд хийдэг байсан хэрэглэгчид онлайнаар гүйцэтгэхэд найдвартай итгэж болохуйц болсон. Иргэдийн бүртгэл болон өмчлөх эрх зэрэг уламжлалт үйлчилгээнүүд бүгд онлайн горимд хийгдэж баталгаажих боломжтой. Банкны гүйлгээ жишээ нь мөнгө шилжүүлэх, орлого зарцуулалт зэрэг хугацаа их шаарддаг ажлуудыг бараг агшин зуурд хийдэг болсон. Аюулгүй, дижитал гүйлгээний бичилт нь дэлхийн эдийн засгийн хувьд асар их ач холбогдолтой зүйл юм.

Анхны блокчэйн апликэйшнууд өөрийн давтагдашгүй токеноор гүйлгээг баталгаажуулж найдвартай дижитал утгыг гүйлгээгээр дамжуулах нөхцөлөөр хангахаар загварчлагдан бүтээгдэж байсан. Үүнд мөнгө болон хөрөнгийн шилжүүлэлт зэрэг багтдаг. Гэвч блокчэйн сүлжээ нь зөвхөн мөнгөний утгыг дамжуулахаас хол давсан боломжит ирээдүйтэй технологи юм.

2.1.5 Блокчэйний бүтэц

Блокчэйн үндсэн гурван цөм хэсгээс бүрддэг :

- **Блок** : Өгөгдсөн хугацаанд гүйлгээний жагсаалт дансанд бичигддэг. Хэмжээ, хугацаа болон блок ажиллах хэмнэл нь блокчэйн бүрд харилцан адилгүй байдаг.

  Криптовалиутын шилжүүлгийг баталгаажуулах бичилт хийх нь блокчэйн бүрийн хувьд нэн тэргүүний зорилт нь байдаггүй ч блокчэйн бүр криптовалиут болон токэн дамжих үйлдлийн бичилтийг хийсээр байдаг. Гүйлгээ гэдгийг энгийнээр мэдээллийн бичилтийг хийх гэж ойлгож болно.

- **Чэйн** : Блокуудыг хооронд нь математикийн ухаанаар хооронд нь холбох хаш утга. Энэ нь блокчэйнийг ойлгоход хамгийн төвөгтэй ойлголт. Чэйн нь мөн блокуудыг нэгтэн байлгаж математикаар итгэл үүсгэж байгаа "шидэт цавуу"юм.

  Блокчэйндэх хаш нь өмнөх блокт байсан мэдээллээс үүсдэг. Хаш нь тухайн мэдээллийг блоктой заавар болон хугацаагаар холбох хурууны хээ болдог.

  Блокчэйн нь хаштай харьцуулахад шинэ нээлт юм. Хаш нь 30аад жилийн өмнө бүтээгдсэн. Энэ эртний технологи шинэ технологитой хоршин ажиллаж байгаа шалтгаан нь хаш нь нэг чиглэлт тайлагдах боломжгүй шифр үүсгэдэг. Хаш

функц нь мэдээллийг математикийн алгоритм ашиглан ямар ч хэмжээтэй байсан хамаагүй тогтсон хэмжээтэй бит стрингс хэлбэрт оруулдаг. Бит стрингс нь ихэвчлэн 32 тэмдэгтийн урттайгаар мэдээлэл хашлагдсан гэдгийг илэрхийлэхүйц бичиглэлтэй болсон байдаг. Secure Hash Algorithm (SHA) нь блокчэйнд ашиглагддаг криптографын хаш функцийн нэг юм. SHA-256 хамгийн өргөн ашиглагддаг бараг л дахин давтагдашгүй 256битийн (32байт) -н тогтсон хэмжээт хаш үүсгэдэг. Практик хэрэглээнд хашийг блокчэйнд мэдээллийг байршуулахад ашигладаг дижитал хурууны хээ гэж ойлгож болно.

- **Сүлжээ** : Сүлжээ нь бүрэн зангилаа(Full node)-уудын хэлхээнээс бүрдэнэ. Бүрэн зангилаа гэдгийг сүлжээний эрсдэлийг хариуцах зориулалттай компьютерт ажиллах алгоритм гэж ойлгож болно. Зангилаа бүр тухайн блокчэйнд хийгдэж байсан болон хийгдэж буй бүх гүйлгээний бичилтийг хадгалж байдаг.

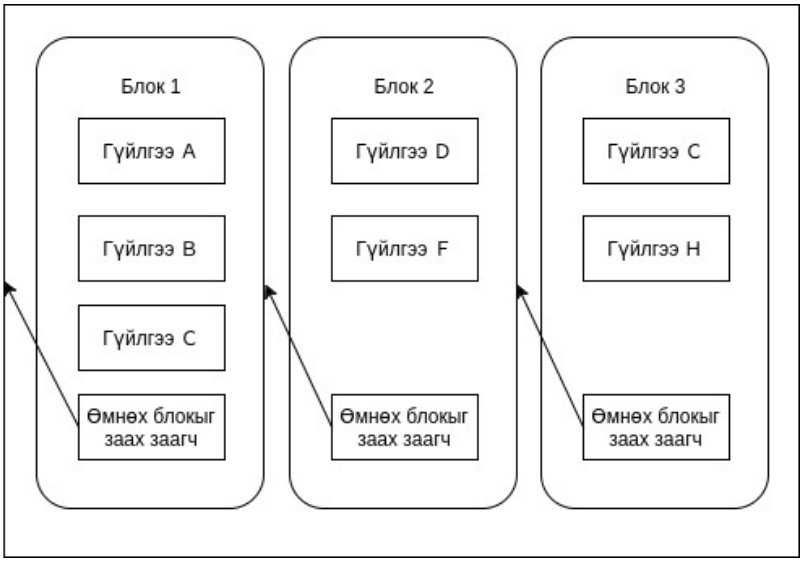
  Зангилаанууд нь хэн ч байж болох бөгөөд дэлхий даяар тархан байрласан байдаг. Бүрэн зангилааг ажиллуулах нь хүндрэлтэй, өртөг өндөртэй мөн цаг хугацаа их шаардсан ажил тул зангилаа болох хэрэглэгчид үүнийг үнэгүй хийдэггүй. Тэд криптовалиут олж авахын тулд зангилааг өөрсдийн компьютер дээрээ ажиллуулдаг. Блокчэйний суурь алгоритм нь зангилаануудад үйлчилгээ үзүүлснийх нь төлөө урамшуулал олгодог. Урамшуулал нь Bitcoin гэх мэт токен болон криптовалиут байдаг.

Bitcoin болон блокчэйн гэх ойлголтуудыг ихэвчлэн бие биеэр нь орлуулж нэг утгаар ашигладах байдал их гардаг, гэвч энэ хоёр нь тусдаа ойлголт юм. Bitcoin өөрийн блокчэйнтэй. Bitcoin-ий блокчэйн нь bitcoin-ий гүйлгээг найдвартай амжилттай хийгдэх зорилго бүхий суурь алгоритм юм. "Bitcoin"нь Bitcoin сүлжээнд ажиллаж буй криптовалиутын нэр бол "Блокчэйн"нь нэг төрлийн програм хангамж юм.

2.1.6 Блокийн гинж (чэйн)

Блокчэйнд энэ шилжүүлгийг гүйлгээ(transaction) гэж нэрлэдэг бөгөөд, олон гүйлгээг багцалсныг блок гэж нэрлэдэг. Гүйлгээ нэг бүрийг зүгээр бүртгээд явбал, нэг мөнгө давхар ашиглагдах “Double spending” хэмээх асуудал үүсдэг. Жишээ нь Батын дансанд 1000 төгрөгийн үлдэгдэл байсан гэе. Нэг зангилаа дээр Батын 1000 төгрөгийг Доржид төлөхөөр боллоо гэж үзье. Гэтэл үүнтэй зэрэгцээд өөр зангилаа дээр Бataас Болдод

1000 төгрөг төлөхөөр боллоо гэж үзье. Зангилаа тус бүр Батын дансны үлдэгдлийг 1000 гэж үзэх учраас, Дорж болон Болд уруу төлөх төлөлтийг зөв гэж үзээд гүйцэтгэчихнэ. Батад 1000 төгрөг л байсан боловч, 1000 төгрөгийг 2 удаа ашиглаад 2000 төгрөг ашигласан болж таарна. Энэ асуудлаас зайлсхийхийн тулд гүйлгээ тус бүрд дараалал өгөх шаардлага гарч байна. Жишээ нь Доржид төлөх төлөлт Болдод төлөх төлөлтөөс "өмнө" хийгдсэн гэж үзвэл, Болдод төлөх үлдэгдэл хүрэлцэхгүй учраас төлөлт хийгдэхгүй. Блокчэйнд блокийг цаг хугацааны дагуу жагсааж, блок тус бүр 1 өмнөх блокийг зааж байдаг(Блокийн гинж). Ийм байдлаар блокийг нэг эгнээнд оруулсан бүтцээс блокчэйн гэдэг нэр үүсэлтэй юм.



Зураг 2.2: Блокийн гинж буюу чэйн

2.1.7 Блокчэйний хөгжлийн үе шат

Блокчэйн bitcoin үүсэхтэй зэрэгцэн үүсэн хөгжсөн. Энэхүү сүлжээнд хоорондоо хэзээ ч уулзаж байгаагүй бүлэг хүмүүс нэг системд бие биедээ итгэн хамтран ажиллаж болдог гэдгийг нотолсон.

Анхны Bitcoin сүлжээ нь Bitcoin криптовалиутын найдвартай байдлыг хангахаар бүтээгдсэн. Дэлхийгээр төвлөрсөн бус 5000 орчин бүрэн зангилаанаас бүрдэж байсан бөгөөд bitcoin арилжаалах болон утга шилжүүлэхэд гол зорилго нь оршиж байсан ч хэрэглэгчид энэ сүлжээнд үүнээс ч илүү боломж байгааг олж харсан. Сүлжээний далайц

болон аюулгүй байдал зэргээс шалтгаалж бусад жижиг блокчэйнүүд болон блокчэйн аппликэйшнуудыг хамгаалахад ашиглагдах болсон.

Ethereum сүлжээ нь блокчэйн концепцын хоёр дахь хөгжлийн үе юм. Уламжлалт блокчэйн бүтцийг ашиглахаас гадна үүн дотор програмын хэл оруулж өгсөн. Bitcoin - той адилаар дэлхийгээр төвлөрсөн бус 5000 орчим бүрэн зангилаанаас бүрдэнэ. Ethereum -ийн үндсэн зорилго нь Ether - г арилжаалах, ухаалаг гэрээ (smart sontract) хийх, төвлөрсөн бус автомат байгууллага(DAOs) бүтээх байсан. Bitcoin - ий адилаар жижиг блокчэйнүүд болон блокчэйн аппликэйшнүүдийн найдвартай байдлыг хангахад мөн ашиглагддаг.

Factom сүлжээ нь блокчэйн технологийн гурав дахь үе юм. Санал хураалтын систем агуулсан, мөн илүү их хэмжээний мэдээлэл агуулах багахан хэмжээний нэгдмэл сүлжээг ашигладаг. Мэдээлэл болон системийн аюулгүй байдлыг хангах зорилгоор бүтээгдсэн. Нэгдсэн зангилаанууд болон хязгааргүй тооны хянагч зангилаатайгаар ажилладаг. Сүлжээ нь жижиг тул төвлөрсөн бус сүлжээнд холбогдож хадгалагч блокчэйнүүдээ холбон ажилладаг.

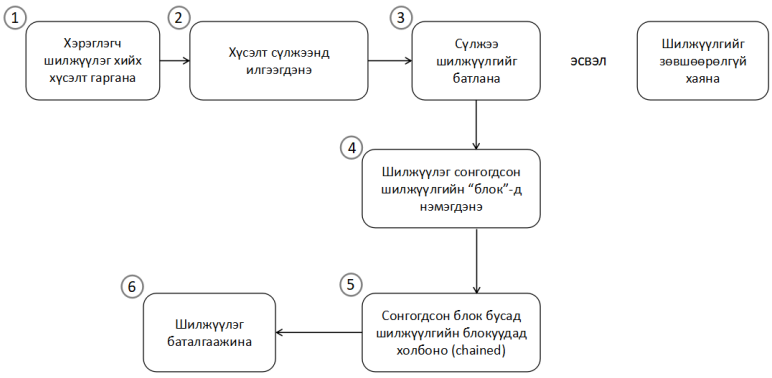
2.1.8 Тохиролцооны алгоритм

Блокчэйн нь системийн дүрмийг хэрэгжүүлэхэд гуравдагч этгээдийн оролцоо шаардлагагүй найдвартай систем юм. Сүлжээний дүрмийг хэрэгжүүлэхэд үндсэн тохиролцооны (concensus) алгоритмыг ашигладаг.

Блокчэйний хувьд үндсэн тохиролцоо гэдэг нь итгэмжлэгдээгүй зангилаануудын хооронд тохиролцоо үүсгэх процесс юн. Тэдгээр нь сүлжээний бүрэн зангилаа (full nodes) байдаг бөгөөд дансны нэг хэсэг болон бичигдэж байгаа гүйлгээ бүрийг баталгаажуулдаг.

Блокчэйн бүр сүлжээндээ өгөгдөл оруулахад тохиролцоо үүсгэх алгоритмтай. Блокчэйн бүр өөр төрлийн өгөгдөлтэй байдаг тул тохиролцоог үүсгэх олон төрлийн загвар байдаг. Зарим блокчэйнууд нь утга солилцдог бол зарим нь мэдээллийг ангилж, зарим нь систем болон гэрээний аюулгүй байдлыг хангадаг.

Жишээ нь Bitcoin - ний хувьд өөрийн сүлжээн дэх хэрэглэгчдийн хооронд токены утгыг дамжуулдаг. Токенууд нь зах зээлийн ханштай тул гүйцэтгэлийн чадал, далайц, найдвартай байдал, аюул болон алдааны эсрэг байдлын шаардлага нь өндөр байдаг. Bitcoin нь халдагчид гүйлгээний түүхийг өөрчлөх эсвэл токен хулгайлахыг оролдох



Зураг 2.3: Блокчэйн хэрхэн ажиллах загвар

зэрэг байнгын аюул дор үйл ажиллагаа явуулдаг. Bitcoin эдгээр аюулаас сэргийлэхийн тулд **"proof of work"** гэж нэрлэгддэг тохиролцоог ашигладаг. Энэ тохиролцоо нь Byzantine - ий үндсэн асуудал болох "Чиний харж байгаа мэдээлэл дотоод болон гадаад талаасаа өөрчлөгдөөгүй гэдгийг яаж мэдэх вэ?"гэдэгт шийдэл болдог. Мэдээлэлд өөрчлөлт оруулах, гуйвуулах асуудал нь компьютерын шинжлэх ухаанд аль ч үед бараг л хэзээд боломжтой асуудал байсаар ирсэн.

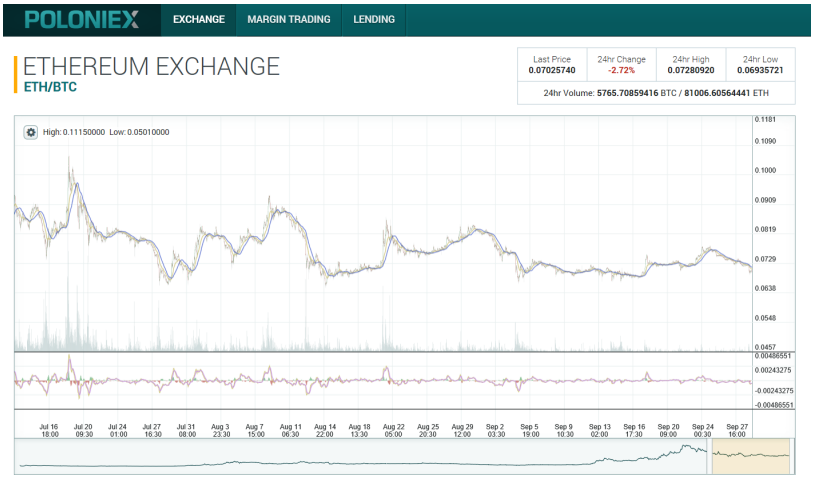
Ихэнх блокчэйнууд гадаад нөлөөлөл болон системийн дотоод хэрэглэгчдээс халдлагад өртөх магадлалын дор ажиллаж байдаг. Ирж болох халдлагууд болон хэрэглэгчдийн сүлжээний найдвартай байдлын зэрэг нь сүлжээнд үйл ажиллагаа явуулж буй зангилаануудын өөрсдийнх нь дансаа тохируулахдаа сонгон ашигласан тохиролцооны алгоритмаас хамаардаг. Жишээ нь Bitcoin болон Ethereum өөрсдийгөө халдлагад өртөх өндөр магадлалтай гэж үзвэл **"proof of work"** алгоритмыг ашиглаж болно.

Нөгөө талаас баталгаажсан цэгүүдийн хооронд мөнгөн гүйлгээний бичилт хийдэг блокчэйнүүд энгийн бөгөөд хурдан ажиллагаатай тохиролцоог ашиглах боломжтой. Тэдний хувьд хурдан хугацаанд гүйлгээ хийх нь илүү чухал. Proof of work нь тэдний хувьд сүлжээнд нь харьцангуй цөөн хэрэглэгч байхаас гадна гүйлгээ бүр шуурхай хийгдэх шаардлагатайгаас шалтгаалж үйл ажиллагаа явуулахад хэтэрхий удаан бөгөөд зардал өндөртэй.

2.1.9 Блокчэйн хэрэглээнд

Өнөөдөр дэлхий даяар маш олон блокчэйн болон блокчэйний апплицэйшнүүд оршиж байна. Дэлхий нийтээр мөнгөний гүйлгээг шуурхай хийх, төвлөрсөн бус сүлжээнд хувь

нийлүүлэх болон удирдах, мөн аюулгүй техник хангамж болон аппликэйшн бүтээхэд анхаарлаа хандуулж байна.



Зураг 2.4: Криптовалиут арилжааны платформ

Блокчэйнууд дан ганц арилжааны утга дамжуулахаас давж бүх төрлийн салбарт оролцож эхэлсэн. Блокчэйн өмнө нь байгаагүй найдвартай байдлыг онлайнд ажиллах орчинд үүсгэж байна.

2.1.10 Өнөөгийн блокчэйний хэрэглээ

Өнөөдрийн ихэнх амжилттай ажиллаж байгаа блокчэйн аппликэйшнууд нь түргэн шуурхай, хямд өртгөөр мөнгө болон бусад төрлийн утга дамжуулах зориулалттай аппликэйшнууд байна. Үүнд хувьцаат компаниудын хувьцаа арилжаалах, олсон улсын ажилчдадаа цалин өгөх, мөн нэг мөнгөн тэмдэгтийг өөр мөнгөн тэмдэгтээр солих зэрэг багтана.

Блокчэйн мөн програм хангамжийн аюулгүй байдлын багцын хэсэгт ашиглагдаж байна. Америкийн бүс нутгийн аюулгүй байдлын яам (U.S Department of Homeland Security) Зүйлсийн Интернет(Internet of Things) - н аюулгүй байдлыг хангах блокчэйн програмуудыг санхүүжүүлж байсан. Зүйлсийн интернет нь гаднаас чагнах болон бусад төрлийн халдлагад өртөх өндөр магадлалтай байсан тул блокчэйн технологиос хамгийн их боломж хүртсэн салбаруудын нэг болсон юм. Зүйлсийн интернет төхөөрөмжүүд илүү сайжирч, аюулгүй байдал нь үлэмж баталгаажсан. Тэдгээрийн жишээ нь эмнэлгийн

систем, өөрийгөө жолоодох машин, болон аюулгүй байдлын системүүд юм.

DAO нь мөн маш сонирхолтой шинэ санаануудын нэг юм. Энэ төрлийн блокчэйн аппликэйшнууд нь компаниудыг онлайнаар нэгтгэн зохицуулах шинэ шийдэл болсон. DAO өмнө нь Ethereum сүлжээгээр зохицуулалт болон хөрөнгө оруулалтаа хийдэг байсан.

2.1.11 Блокчэйн аппликэйшн ирээдүйд

Улсын хэмжээнд газрын бүртгэл хийх, иргэдийн бүртгэл болон олон улсын зорчигч тээврийн аюулгүй байдлыг хангах програмуудын туршилт дээрх томоохон урт хугацааны судалгааны ажлууд хийгдэж байна. Их Британи, Сингапур, Арабын Нэгдсэн Эмират Улс зэрэг орнууд блокчэйнийг зардал бууруулсан шинэ төрлийн эдийн засгийн хэрэгсэл гэдэг талаас нь харж байгаа бөгөөд идэвхтэй хөрөнгө оруулалт болон судалгаа хийсээр байна.

Математик тэгшитгэлээр "итгэлцэл"гэх зүйл үүсгэснээр блокчэйн шаардлагатай салбаруудаа хүрч чадсан. Өмнө нь "итгэлцэл"гэх зүйл нь зарим салбарт ахадсан зүйл байсан бол блокчэйн үүссэнээр энэ нь байх боломжтой зүйл болсон. Түүнчлэн "итгэлцэл"гэх зүйл үгүй болсон газарт дүрэм сахиулах салбарынхны ажлыг хөнгөвчилсөн. Утгат суурилсан болон нийгэмд суурилсан гүйлгээг бид хэрхэн хийж байгаагаас хамаарч блокчэйн өөрчлөгддөг тул блокчэйн аппликэйшны нийгмийн болон эдийн засгийн ойлголт нь сэтгэл хөдлөлийн болон улс төрийн туйлшралд өртөж байна.

2.1.12 Блокчэйнийг хүрээлэн буй орчин

Аппликэйшн хөгжүүлэлтийн гол талбар байгууллага доторх компьютероос (on-premise software) үүлэн технологи (cloud) уруу шилжсэнтэй адилаар, блокчэйнийг бас хэд хэдэн үүлэн орчинд ашиглах боломжтой.

Голлох үйлчилгээ нь IBM-н хөгжүүлж буй Hyperledger-ийн үүлэн үйлчилгээ “IBM Bluemix Blockchain” болон Microsoft-ийн үзүүлдэг Ethereum үүлэн үйлчилгээ “Microsoft Azure Blockchain as a Service (BaaS)”, Sakura Интернетийн Tech Bureau-тай хамтран үзүүлдэг NEM-д суурилсан mijin үүлэн үйлчилгээ “mijin cloud service beta” зэрэг юм.

Аль ч үйлчилгээ нь, хугацааны хувьд харилцан адилгүй ч, тодорхой хэмжээнд үнэгүй ашиглах боломжтой учраас блокчэйн ашиглаж үзье гэвэл энэ мэт үүлэн үйлчилгээнүүдийг ашиглах боломжтой.

Цаашид иймэрхүү чиглэлийн үйлчилгээ улам эрчимжиж, блокчэйнийг хүрээлсэн орчин улам бүр төгөлдөржих байх гэж харагдаж байгаа.

2.1.13 Технологи болон хууль, эрх зүй

Блокчэйний хөгжүүлэлт хийх орчин улам төгөлдөржихийн хамт, хийсвэр мөнгө талаасаа, харамсалтай нь мөнгө угаалтанд ашиглагдах, гэмт хэрэгт ашиглагдах зэрэг нь мөн ихэссээр байна. 2016 оны 5 сард Японд хийсвэр мөнгөний тухай хууль батлагдсан.

Уг хууль хэрэгжиж эхлэхээр, хийсвэр мөнгө "Төлбөрийн хэрэгсэл болгон ашиглаж болох хөрөнгө" гэж тодорхойлогдсон бөгөөд (ердийн марк болон кредит карттай адилаар) хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үед татвар ногдуулахгүй болох юм.

Мөн уг хуульд, хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үйл ажиллагааг бүртгүүлсэн хуулийн этгээд явуулах бөгөөд суурь хөрөнгийн талаарх шаардлага болон үйл ажиллагааны явц дахь мэдээллийн хяналт, тогтмол шалгалт зэргийг нарийн дүрмүүдээр зааж өгсөн байна.

2.1.14 Блокчэйний боломжууд

Блокчэйнийг цаашид ямар салбарт хэрэглэгдэхээр харагдаж байгаа талаар танилцуулъя. Эхний хэрэглээний салбар бол, bitcoin гол төлөөлөл нь болж буй криптовалиут юм.

Уламжлалт банк санхүүгийн байгууллагаар дамжуулж гүйлгээ хийх нь төвөгтэй шат дамжлагатай мөн шимтгэл өндөртэй, хугацаа их шаарддаг. Блокчэйн ашигласан хийсвэр мөнгөний хувьд ийм дундын зуучлагч шаардахгүйгээр гүйлгээ хийх боломжтой бас гүйлгээний шимтгэл бага, цаг хугацаа хэмнэдэг. Ялангуяа улс хооронд мөнгө илгээхэд дээрх давуу талуудыг мэдрэх болно. 2015 оны байдлаар, дэлхий даяар илгээж буй мөнгөн дүн ойролцоогоор 60 их наяд иентэй дүйцэхүйц том зах зээл байна.

Дараагийн салбар нь баримт бичгийн баталгаажуулалт (нотариат) юм. Засах боломжгүй гэдэг шинж чанарыг ашиглан, блокчэйн дээр баримт бичиг, эсвэл баримт бичгийн хаш утгыг хадгалснаар, тэрхүү баримт бичиг нэг цаг үед байсан, мөн тухайн үеийн агуулга нь өөрчлөгдөөгүй гэдгийг баталж чадна.

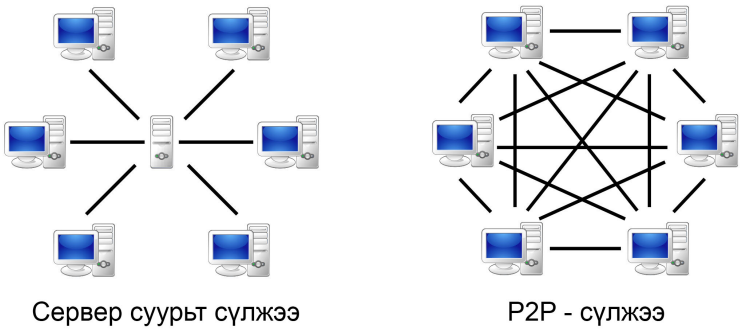
Эстониа улсад, гэрлэлтийн баталгаа, гэрээслэл, газар эзэмшлийн гэрчилгээ зэргийг блокчэйнд хадгалснаар, уламжлалт нотириатыг орлох оролдлого хийж байна. Мөн тус

улсад хувь хүний эмчилгээний түүх үрүү хандах хандалтад блокчэйнд суурилсан технологийг ашиглаж байна.

Технологиос гадна, хууль эрх зүйн хүрээнд ч бас өөрчлөлт орж байна. Ялангуяа Fintech-ийн хувьд олон компани хүчээ үзэж байна.

2.2 Төвлөрсөн бус сүлжээ (Decentrelized network)

Компьютеруудыг хэрэглэх хандлага зонхилох үед персонал компьютерууд дотоод сүлжээгээр дамжин төв сервертэй холбогддог байсан. Эдгээр серверүүд маш их өгөгдөл боловсруулдаг учир персонал компьютероос хүчин чадлын хувьд маш өндөр байсан. Түүнээс хойш персонал компьютер хүчирхэг болсоор ойр орчмын төв серверүүдээс өгөгдлийг боловсруулахдаа илүү болсон. Яагаад гэвэл PC-ээс PC-рүү эсвэл төвлөрсөн бус тооцоолол нь хувийн компьютерыг төв серверийг тойрч бусад компьютеруудтай шууд хамтран ажиллах боломжийг хангаж чаддаг. Клиент серверийн аль аль нь хүсэлт илгээх эсвэл үйлчилгээ үзүүлэх эсэхээс хамаардаг бол төвлөрсөн бус систем дэх бүх зангилааг зиндаа нэг гэж авч үздэг. Өөрөөр хэлбэл нэг клиент нь нөгөөгөөсөө мэдээлэл авч байхад нөгөө клиент эргүүлээд мэдээлэл тэгш эрхтэйгээр өгч байна гэсэн үг юм.



Зураг 2.5: Peer to peer сүлжээ болон сервер суурьт сүлжээний топологи

3 н төрлийн төвлөрсөн бус тооцоолол байдаг. Үүнд:

- **Олон тооны компьютерын харилцаа холбоо** - Персонал компьютерууд бусад серверүүдээр дамжин сүлжээнд холбогдож, файлуудыг хадгалж хуваалцаж мөн

ижил сүлжээн дэх хэн нэгнээс авдаг. Нэг гол асуудал нь энэ нь аюулгүй байдлын хамгаалалт болон оюуны өмчийн асуудлыг авчирдаг.

- **Хуваалттай харилцаа холбоо** - Бүлэг компьютерууд тэдгээрийн тооцоолол болон интернетээс хайлт хийж боловсруулах, асар их процессыг шийдвэрлэх асуудлыг тооцоолохын тулд нэгдэж хамт сүлжээнд холбогддог.

- **Хамтарсан харилцаа холбоо** - Багахан хэмжээний бүлэг хүмүүс ижил интерфэйсээр дамжин харилцах. Жишээ нь: Тоглоом тоглох, чатлах, шуурхай мессеж, алсын зайнаас суралцах орчин гэх зэрэг.

Төвлөрсөн бус тооцооллын систем нь peer-to-peer сүлээнд ажилладаг. Төвлөрсөн бус P2P сүлжээ гэдэгт, сүлжээнд оролцогч буюу зангилаа нь газарзүйн хувьд тархсан байдаг ба зангилаа хооронд мэдээлэл солилцоо нь агшин зуур хийгддэггүй, тархах байдлаар явагддаг учраас “төвлөрсөн бус” гэдэг утгыг, мөн зангилаа нь сервер зэргээр дамжилгүйгээр өөр зангилаа-тэй шууд холбогддог “P2P(peer to peer)” гэдэг утгыг агуулж байдаг.

Төвлөрсөн бус P2P сүлжээнд гүйлгээг баталгаажуулахын тулд, зангилаа хоорондын мэдээлэл солилцоо шаардлагатай болно. Дээрх мөнгө шилжүүлэх жишээн дээр мөнгө шилжүүлэлт зөв явагдсан эсэхийг баталгаажуулахын тулд, хэнд хэчнээн төгрөг байгаа вэ гэдэг мэдээллийг сүлжээнд байгаа бүх зангилаа дээр мэдэж байх хэрэгтэй.

Тодорхойгүй тооны олон оролцогчтой сүлжээнд, мэдээллийг солилцохдоо, тэдгээр мэдээллийг засах эрсдэлтэй биш үү, ялгаатай зангилаа дээр ялгаатай үр дүнд хүрвэл яаж нэгдсэн нэг үр дүнд саналаа нэгтгэх вэ гэдгийг бодох шаардлагатай гарч байна.

Peer-to-peer сүлжээ нь голдуу физик сүлжээний топологи дээр виртуал бүрхэх сүлжээний (Overlay network) зарим загварыг хэрэгжүүлдэг. Мэдээллүүд үндсэн TCP/IP сүлжээн дээгүүр дамжуулагдсаар байдаг ч application layer-т peer-үүд логик бүрхэх холбоосоор хоорондоо шууд холбогдож харилцдаг. Давхаргууд нь peer олох болон индексжүүлэх, мөн P2P системийг физик сүлжээний топологиос хамааралгүй болгоход ашиглагддаг. Зангилаанууд давхарга сүлжээгээр бие биетэйгээ хэрхэн холбогдсон байдал, мөн нөөцүүд хэрхэн индексэжсэн болон байршсан байдлаас шалтгаалж бүтэцлэгдсэн болон бүтэцлэгдээгүй сүлжээ гэж ангилдаг(эдгээр хоёрын хосолмол бүтэцтэй байдаг). Gnutella, FastTrack гэх мэт P2P сүлжээнүүд нь бүтэцлэгдээгүй сүлжээ юм.

Төвлөрсөн бус сүлжээ нь дараах давуу талуудтай

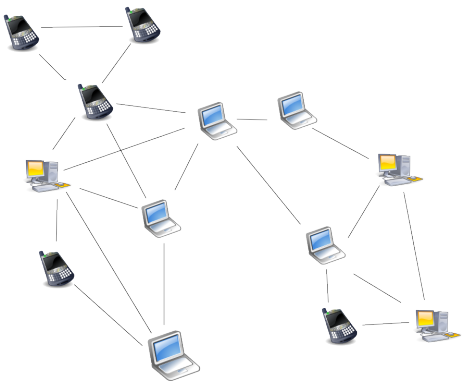
- Суурилуулах болон тохируулахад хялбар
- Холбогдсон компьютерууд нь серверээс хамаарахгүй
- Хувь хэрэглэгчид өөрсдийн хамтран хуваалцаж буй эх сурвалжийг хянаж чадна
- Худалдан авах болон байгуулахад үнэтэй биш
- Сүлжээний тусгай програм хангамж шаарддаггүй
- Сүлжээнд ажиллах тусгай администратор шаардахгүй

Төвлөрсөн бус сүлжээ нь дараах сул талуудтай

- Сүлжээний хамгаалалт нь зөвхөн тухайн эх сурвалжид тухайн цаг хугацаанд хамаарна
- Хэрэглэгчид эх сурвалж болгонд өөр өөр олон нууц үг өгдөг.
- Холбогдсон компьютер болгон өөрийн эх сурвалжаа хамгаалах шаардлагатай

2.2.1 Unstructured nertwork

Structured буюу бүтэцлэгдээгүй peer-to-peer сүлжээ нь загварын хувьд бүрхэх сүлжээн дээр тодорхой бүтцийг байгуулдаггүй, харин зангилаанууд хоорондоо санамсаргүй байдлаар холболт үүсгэж зохион байгуулалтад ордог. (Gnutella, Gossip, Kazaa зэрэг нь бүтэцгүй P2P протоколын жишээ юм)



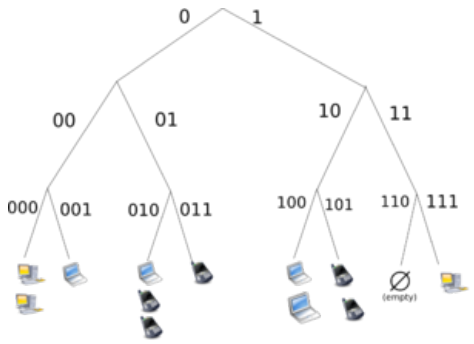
Зураг 2.6: Бүтэцлэгдээгүй сүлжээний загвар

Бүтэцлэгдээгүй сүлжээнүүдийн дээгүүр дахин шинэ бүтэц нэмэгдэхгүй тул байгуулахад амар бөгөөд давхаргын өөр өөр байршилд зохион байгуулах боломжтой. Түүнчлэн сүлжээн дэх бүх peer-үүдийг үүрэг оролцоо ижил учир бүтэцлэгдээгүй сүлжээ нь маш олон тооны peer-үүд ойр ойрхон сүлжээнд холбогдох болон гарах үе гэх мэт ачаалал өндөртэй үед маш бат бөх байж чаддаг.

Бүтцийн дутагдалтай байдлаас шалтгаалж бүтэцлэгдээгүй сүлжээнд зарим хязгаарлагдмал байдлууд бий болдог. Тухайлбал, сүлжээн дэх peer мэдээллийн тодорхой нэг хэсгийг олох хэрэгцээ гарвал, хайлтын хүсэлт сүлжээн дэх тухайн мэдээллийг агуулж болох аль болох олон peer - үүдээр урсаж гарна. Энэ урсгал нь сүлжээнд маш их хэмжээний сигналын ачаалал үүсгэж CPU/memory - н ачааллыг нэмэгдүүлдэг ч хайлтын хүсэлт үргэлж амжилттай биелнэ гэсэн баталгаа байдаггүй. Түүнчлэн peer-үүдийн хооронд ямар ч харилцан хамаарал байдаггүй тул тухайн хайлтын урсгал хүсэж буй мэдээлэл нь хадгалагдаж байгаа peer-ээ олно гэх баталгаа мөн байдаггүй. Олон peer-үүдэд хадгалагдаж буй түгээмэл файлууд олдох магадлал өндөр байдаг бол хэдхэн peer-т байгаа мэдээллийг хайхад олдох үр дүн маш бага байдаг.

2.2.2 Structured network

Structured буюу бүтэцлэгдсэн сүлжээ нь давхарга тодорхой топологи болох зохион байгуулагддаг, мөн протокол нь сүлжээнд аль ч peer хүссэн файл болон нөөцийг хэдий маш ховор байсан ч үр ашигтайгаар хайж олох баталгааг хангадаг.



Зураг 2.7: Бүтэцлэгдсэн сүлжээний загвар

Хамгийн өргөн ашиглагддаг бүтэцлэгдсэн P2P сүлжээний төрлүүд нь хайж байгаа мэдээллээ хэн эзэмшиж байгааг тодорхойлох зорилгоор ашигладаг бүрэлдэхүүнт хаш

(consistent hashing) - н төрөл болох distributed hash table (DHT) - г ашигладаг. DHT - д хадгалагдаж буй хослол(түлхүүр, утга)-н hash table - г ашиглан сүлжээний нөөцийг олох боломжтой болгодог, мөн ямар ч идэвхтэй зангилаа үр ашигтайгаар өгөгдсөн түлхүүрт нийцэх утгыг буцаана.

Сүлжээний үр ашигтай байдлыг хангахын тулд бүтэцлэгдсэн сүлжээн дахь зангилаанууд тухайн нөхцөлийг хангасан хөршийн жагсаалтыг дэмждэг байх ёстой. Ингэснээр сүлжээний өндөр ачаалалтай үед зангилаануудыг тэсвэр багатай болгодог. Бодит ачааллын үе дэх P2P нөөц олох шийдэлд хийсэн тооцооллоор нөөц зарлах/илрүүлэх ачаалал өндөр, мөн статик болон динамик ачааллын тэнцвэр алдагдах зэрэг DHT - д суурилсан хэд хэдэн асуудлыг илрүүлсэн.

2.2.3 Hybrid model

Hybrid буюу хосолмол загвар нь peer-to-peer сүлжээ болон клиент-сервер загварын хослол юм. Нийтлэг хосолмол загвар нь peer-үүд нэг нэгнээ олоход зориулагдсан төвлөрсөн сервертэй байдаг. Энэ төрлийн загварын томоохон жишээ нь Spotify юм. Маш олон тооны хосолмол загварууд байдаг бөгөөд тэдгээр нь бүгд бүтэцлэгдсэн клиент/сервер сүлжээгээр загварчлагдсан төвлөрсөн үйл ажиллагаагаар тохиролцож, харин peer-үүд бүтэцлэгдээгүй цэвэр peer-to-peer сүлжээгээр хангагддаг. Одоогийн байдлаар хосолмол загвар нь төвлөрсөн үйл ажиллагаат хайлттай бөгөөд зангилаанууд нь бүтэцлэгдээгүй сүлжээний төвлөрсөн бус үйл ажиллагааны давуу талыг ашигласан нь цэвэр бүтэцлэгдсэн болон цэвэр бүтэцлэгдээгүй сүлжээний загваруудаас харьцангуй илүү гүйцэтгэлтэй байж чадаж байна.

2.3 Нууцлал аюулгүй байдал

2.3.1 Хаш функц

Хаш функц нь блокчэйн технологийн үндсэн суурь хэсэг юм. Хэрэв хаш функцийг ойлгочихвол хорт үйлдлийг илрүүлэх (tamper proof), тоон хурууны хээ зэрэг бусад концепцуудыг ойлгоход хялбар болно.

Хаш концепц нь үнэндээ маш энгийн. Энэ технологийг тайлбарласан техникийн хэл нь л хүмүүсийн толгойг эргүүлдэг. Хаш функцийг энгийнээр тайлбарлавал энэ нь тодорхой нэг оролтын утгыг авч гаралтын утга үүсгэдэг функц юм.

Энэ тодорхойлолтыг дэлгэрүүлбэл, хаш функц ямар ч хэмжээтэй утгыг оролтдоо аваад тогтмол урттай гаралтын утга үүсгэдэг.

MD5 гэж нэрлэгддэг хаш функцийн нэг төрлөөр жишээ авъя:

```
cloudnthings:bin cloudnthings$ echo "I owe my sister $5" | md5
a0680c04c4eb53884be77b4e10677f2b
cloudnthings:bin cloudnthings$
```

Зураг 2.8: MD5 -аар хашлах үйлдэл

Үүнд авсан стрингс утгаа санамсаргүй тоо болон үсгээс бүрдсэн “a0680c04c4eb53884be77b4e1067
гэх гаралтын утга болгон гаргасан байна. Энэ үйлдлийг **мэдээллийг хураангуйлах** (message digest) гэж нэрлэдэг. Түүнчлэн **тоон хурууны хээ** ч гэж нэрлэгдэх нь бий. Дээрх жишээн дэх “I owe my sister $5” гэсэн оролтын утгын зөвхөн ганц тэмдгийг өөрчлөх буюу жишээ нь “I owe my sister $2” болгоход гаралтын утга нь тэр чигтээ өөрчлөгдөх болно.

2.3.2 Хаш функцийн төрлүүд

Олон төрлийн хаш функц байдаг. Блокчэйний хувьд үндсэн ашигладаг хаш функц нь SHA256 болон RIPEMD. 128 эсвэл 256 гэх тоонууд нь үндсэндээ гаралтынхаа утгын уртыг илэрхийлдэг. SHA256 нь 256бит утга гаргана гэсэн үг.

```
pi@raspberrypi:~ $ echo -n "I owe my sister $5" | sha256sum
5d0838314e62443e929c6794a0d2a566a23a69fa614243bfe20e8ca651e955b0
```

Зураг 2.9: SHA256 гаралтын утга

Дээрх зурагт SHA256 командыг Линукс дээр ажиллуулаад гаралтдаа 256ит буюу 64 тэмдэгтийн урттай болсон байна.

2.3.3 Өөрчлөлтийг илрүүлэх

Ирсэн мэдээллийг замдаа өөрчлөгдсөн эсэхийг мэдэх хамгийн амар арга нь илгээгчийн мэдээллийн гаралтын хаш утгыг ирсэн мэдээллийн хаш утгатай харьцуулах юм. Хэрэв хаш утгууд яг ижил байвал мэдээлэл алдаагүй иржээ гэдэгт итгэлтэй байж болно.

2.3.4 Давхцал

Маш олон хүмүүс мэдээллийн хураангуй хэзээ ч давхцахгүй байх боломжтой юу гэдэгт эргэлзэн, хэзээд дахин давтагдашгүй байна гэдэг боломжгүй гэж үздэг.

Мэдээж гаралтын утга тогтсон урттай тул хязгааргүй тооны дахин давтагдашгүй утга байна гэж байхгүй ч энэ технологийн нууц нь хоёр өөр утга ижил хаш гаралттай байх тохиолдлыг олохын тулд бүх компьютеруудыг ашиглахад хэдэн арван сая жил шаардагдана. Иймд энэ технологи ойрын ирээдүйн хэрэгцээнд хангалттай баталгаатай гэсэн үг юм.

2.3.5 Нэг чиглэлт функц

Өөр нэг хаш функцийн чухал шинж нь нэг чиглэлт үйлдэл хийдэг. Энэ нь мэдээллийг хураангуйлахад маш хялбар боловч хураангуйллыг эргэн тайлах нь бараг л боломжгүй зүйл юм. Өмнөх жишээ шиг мэдээж огт боломжгүй биш боловч гаралтын утгыг олоход мөн л асар их хугацаа шаардана.

2.3.6 Шахалт

Хаш функцийн бас нэг ойлголт нь шахалт. Том хэмжээтэй өгөгдөл стрингсээр илэрхийлэгдэх маш богино өгөгдөл болон гардаг. Үүнийг мэдээлэл дамжуулалтын явцад алдаа гарсан, эсвэл өөрчлөлт орсон зэргийг илрүүлэхэд ашиглаж болдог.

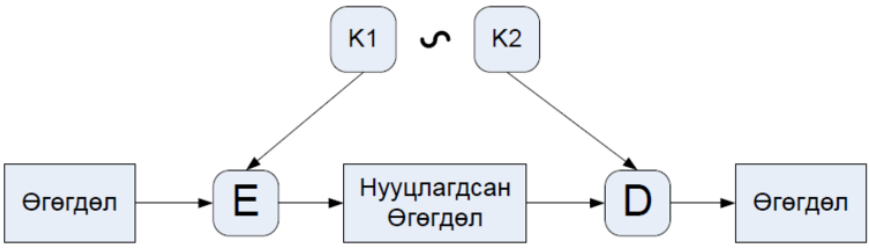
2.3.7 Хаш функц блокчэйнд хэрхэн хэрэглэгддэг вэ

Блокчэйн үйл ажиллагаандаа хаш функцийг байнга ашигладаг. Блокчэйн дахь мэдээллүүд блок бүрд хашлагдсан байдаг. Хэрэв блок өөрчлөгдвөл, жишээ нь хэн нэгэн өөрт байгаа bitcoin -ий хэмжээг өөрчлөх, эсвэл хэн нэгэнд хэр өртэй гэдгээ өөрчлөхийг оролдвол хаш утга нь өөрчлөгдөөд бусад блок бүр ямар нэг өөрчлөлт гарсныг тэр дороо мэднэ.

Өмнөх блокийн хашлагдсан утгыг шинэ блокийн хаш утгыг үүсгэхэд ашигладаг тул блокуудын холбоо үүсдэг.

2.3.8 Нийтийн түлхүүртэй нууцлалын алгоритм

Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компьютерт хадгална.



Зураг 2.10: Нийтийн түлхүүртэй алгоритм

2.3.9 RSA алгоритм

RSA нь интернет дээгүүр хувийн болон нууц мэдээлэл дамжуулахад өгрөн ашиглагддаг нийтийн түлхүүрээр мэдээллийг нууцлах крипто-систем юм. RSA-г 1978 онд Масачүсетийн Технологийн хүрээлэнгийн (Massachusetts Institute of Technology) R.Rivest, A.Shamir, L.Adelman нар бүтээсэн. Нийтийн түлхүүрт шифрлэлт буюу ассиметрик шифрлэлт нь нэг нийтийн болон нэг хувийн хоёр өөр боловч математикийн уялдаатай түлхүүрүүд ашигладаг. Нийтийн түлхүүр нь бүгдэд нээлттэй бол хувийн түлхүүр нь нууц байх ёстой. RSA шифрлэлтэд нийтийн болон хувийн түлхүүрүүд хоёул зурвасыг шифрлэх боломжтой. Энэ шинж нь RSA алгоритмыг хамгийн өргөн ашиглагддаг ассиметрик алгоритм болгосон.

RSA алгоритм нь өнөөгийн мэдээлэл технологийн хамгаалалтын гол тулгуур болж байна. Интернетээр худалдаа хийх үед хөтчийн веб хаягийн өмнөх цоожны зураг онлайн дэлгүүртэй хийж буй харилцаа шифрлэгдсэн байгааг илэрхийлнэ. Цоожны зурган дээр даралт хийж, дэлгэрэнгүй мэдээлэл дотроос тоо болон үсгүүдийн дарааллыг харж

болно. Энэ нь 16-тын тооллоор илэрхийлэгдсэн хэн ч харж болох нийтэд дэлгэсэн түлхүүр юм. Кредит картын дугаарыг оруулах үед нийтэд ил харагдах түлхүүр автоматаар дуудагдаж, дугаарыг шифрлэн дэлгүүрт илгээдэг. Ил түлхүүр үнэхээр аюулгүй байж чадах уу гэсэн эргэлзээ төрнө. Үүний нууц нь зөвхөн нэг чиглэлт функцийн үр дүн юм. Бид телефон утасны жагсаалтаас хүний нэрээр утасны дугаарыг олж болох ч, эсрэгээр дугаараас нэрийг олж болдоггүйтэй адил юм.

RSA алгоритм анхны тоог ашигладаг. Анхны тоо нь 1, 3, 5, 7, 11 гэх мэтчилэн хязгааргүй үргэлжилнэ. Эрдэмтэд 2500 жилийн туршид бүхий л анхны тоог нэгэн зэрэг илэрхийлэх нэгдсэн томьёог хайсаар ирсэн боловч олж чадаагүй л байна. Энэ нь анхны тоог шифрлэлтэд ашиглах үндэс болжээ. Дэлгүүр хэрэглэгчийн мэдээллийг нууцлахын тулд урьдчилан 2 анхны тоог сонгодог. Тэдгээрийн үржвэр нь нийтэд үзүүлэх түлхүүр болно. Кредит картын дугаар энэ түлхүүрээр шифрлэгдэн илгээгдэж, дэлгүүр анхны 2 тоог мэдэх учир шифрийг тайлж кредит картын дугаар уншигдана. Нөгөө талаас хакерууд түлхүүрийг анхны тооны үржвэрт задалж чадвал кредит картын дугаарыг мэдэж чадах мэт санагдана. Гэвч энэ нь боломжгүй юм. Одоогийн байдлаар RSA шифрлэлтийн түлхүүр нийт 617 оронгоос бүрдэж байна. Энэ нь өнөөгийн ямар ч супер компьютер, хэдэн ч ширхгийг ашигласан үржвэрийг олох боломжгүй том тоо юм.

RSA алгоритмыг Америкийн Үндэсний Стандартчиллын Газар (NIST)-аас PKCS1, ANSI X9.31, IEEE 1363 стандартуудаар баталгаажуулсан байдаг бөгөөд мэдээллийн жижиг блокуудыг шифрлэх, түлхүүр солилцох үйлдлийг ашигладаг програм хангамжууд болон SSH, OpenPGP, S/MIME, болон SSL/TLS зэрэг маш олон протоколуудад, мөн тоон гарын үгийн загварт хэрэглэгдэж байна.

RSA алгоритмын түлхүүрийг 512бит, 1024бит, 2048бит, 4096бит урттайгаар сонгон авч болдог. Төсөөлбөл 64, 128, 256, 512 үсэгтэй нууц үг байна гэж ойлгож болно. Ийм урт нууц үгийг цээжлэх хэцүү. Тиймээс нууц үгийг файл дээр бичээд компьютерт хадгалдаг. Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компью-

терт хадгална. RSA алгоритмаар ямар ч хэмжээний өгөгдлийг нууцалж болно. Өгөгдлийг нийтийн түлхүүрээр нууцалж, хувийн түлхүүрээр тайлна. RSA алгоритмын давуу тал нь өгөгдлийг нууцлах болон баталгаажуулах чадвартай байдаг. Нууцлах бол бидний мэддэгээр баримт бичгийг бусад хүмүүс гартаа оруулсан ч унших боломжгүй болгохыг хэлнэ. Харин баталгаажуулах нь баримт бичигт тамга даран баталгаажуулдаг шиг тийм үйлдлийг тоон баримтад хэрэгжүүлдэг. Үүнийг тоон гарын үсэг гэж нэрлэн заншжээ. RSA алгоритмыг тоон гарын үсэг, сертификатад голлон ашиглаж байна.

RSA нийтийн түлхүүр нь (n, e) гэсэн бүхэл тоон хосоос бүрдэх ба энд RSA модуль n нь ижил битийн урттай санамсаргүйгээр үүсгэсэн (нууц) p, q хоёр анхны тоонуудын үржвэр байна. Өөрөөр хэлбэл $n = p * q$. Шифрлэх илтгэгч нь :

$$1 < e < \varphi(n), \;\; ged(e, \varphi(n)) = 1$$

нөхцөлийг хангах бүхэл тоо, энд $\varphi(n) = \varphi = (p-1)(q-1)$. Хувийн түлхүүр d-ийг мөн шифр тайлах илтгэгч гэж нэрлэх ба

$$1 < d < \varphi(n), \;\; ed \equiv (mod\varphi)$$

нөхцөлийг хангах бүхэл тоо байна. (n, e) нийтийн түлхүүрээс хувийн түлхүүр d-ийг тодорхойлох бодлого нь n тооны p, q үржвэрүүдийг тодорхойлох бодлоготой тооцооллын хувьд нэг болохыг баталсан. Аливаа том тоог анхны тоонуудын үржвэрт задлах асуудал нь тооцооллын хувьд хүнд бодлого юм.

2.3.10 Цахим гарын үсэг

Өдөр тутмын амьдралд файл болон бичиг баримтыг илгээж, хүлээж авахдаа чухалчилж бодолгүй гүйцэтгэдэг хүмүүс олон байх. Гэвч, хүлээж авсан файл үнэхээр зөв хүнээс илгээгдэж ирсэн эсэхийг баталгаажуулж чадахгүй байж болох юм.

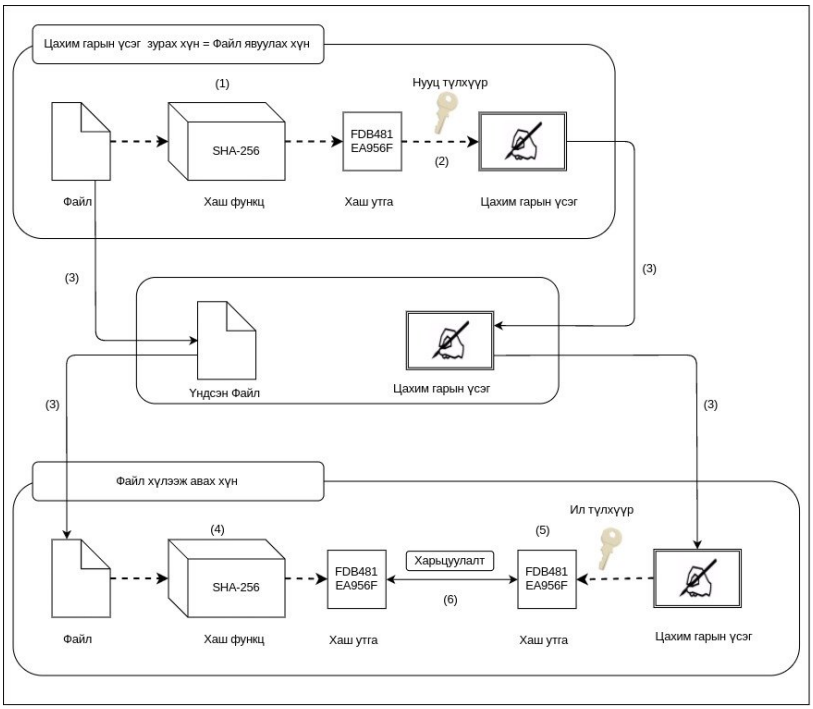
Жишээ нь Бат Доржид чухал материал илгээх тохиолдолд, муу санаатай хэн нэгэн Батын оронд өөр материал илгээж магадгүй, эсвэл Батын явуулсан материалыг замаас нь хулгайлж, засварлаад Доржид явуулж магадгүй. Энэ үед Доржийн хүлээж авсан файл “Бataас илгээсэн зөв файл мөн” гэдгийг хэрхэн шалгах вэ. Энэ асуудлыг шийдэж өгөх арга нь цахим гарын үсэг юм.

Дээрх жишээ шиг олон тохиолдолд файл болон бичиг баримтыг илгээх үед, хүлээж авагч нь тухайн файлыг илгээгч нь үнэн зөв илгээгч байсан, бичиг баримт нь мөн үнэн зөв, засварлагдаагүй байсан гэдгийг баталгаажуулах шаардлагатай.

Цахим гарын үсгээр, түлхүүрийн хослолыг(нууц болон нийтэд ил) ашиглан, гарын үсгийг үүсгэж, гарын үсгийг шалгаснаар дээрх шаардлагыг хангадаг. Нууц түлхүүр нь гарын үсэг гэж нэрлэгддэг бөгөөд, гарын үсэг зурах хүнд л байна. Харин, нийтэд ил түлхүүр нь шалгалтын түлхүүр гэж нэрлэгддэг бөгөөд, хэн ч олж авах боломжтой байдлаар нийтэд ил болгосон байдаг. Нууц түлхүүр болон нийтэд ил түлхүүр нь дараах онцлогуудтай.

- Нууц түлхүүрээр нууцалсан өгөгдлийг зөвхөн ил түлхүүрээр задлах боломжтой
- Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой

Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой Ил түлхүүрээр нууцлах нь “Интернет дэлгүүрт кредит картын мэдээлэл илгээх”, “Нэвтрэх нууц үг илгээх” зэрэгт ашиглагддаг. Харин, нууц түлхүүрээр нууцалсан өгөгдөл нь зөвхөн, нууц түлхүүртэй хүн л нээнэ гэдэг чанарыг ашиглаж “хэн задалсан бэ” гэдгийг нь баталгаажуулах арга(цахим гарын үсэг) болгон ашигладаг. Батаас Доржид бичиг баримт илгээх тохиолдлыг жишээ болгон цахим гарын үсгээр явуулахыг Цахим гарын үсэгтэй файл явуулах урсгал-д үзүүллээ.



Зураг 2.11: Цахим гарын үсэгтэй файл явуулах урсгал

1. Бат (Гарын үсэг зурах = нууц түлхүүртэй хүн) үндсэн файлын хаш утгыг тооцоолно.
2. Батын нууц түлхүүрээр олсон хаш утгыг кодлоод, түүнийг гарын үсэг гэж үзнэ.
3. Батаас үндсэн файл болон гарын үсгийг Доржид илгээнэ.
4. Дорж хүлээж авсан файлаас хаш утгыг нь бодож олно.
5. Дорж хүлээж авсан гарын үсгийг Батын нууц түлхүүрт харгалзах ил түлхүүрээр задалж, үндсэн файлд харгалзах хаш утгыг олж авна.
6. Дорж 4-т бодож олсон "үндсэн файлын хаш утга" болон 5-д задалж олсон "үндсэн файлын хаш утга"-г харьцуулна.
7. Уг харьцуулалтаар 4 болон 5-ууд ижилхэн байвал уг файл Батаас явуулсан файл мөн бөгөөд ямар нэг засваргүйгээр хүлээж авсан гэдгийн баталгаа болно.

Ийм байдлаар, цахим гарын үсэгт хаш функц болон хос түлхүүрийг нийлүүлж ашигласнаар, өгөгдөл илгээгчийг болон агуулгын засагдаагүй гэдгийг баталгаажуулах ажлыг зэрэг гүйцэтгэдэг юм. Блокчэйнд өмнөх хэсгийн хаш функц болон дээр өгүүлсэн цахим гарын үсгийг аль алийг нь ашигладаг бөгөөд гүйлгээ тус бүрийн үнэн зөв байдал, нийцтэй байдлын талаарх мэдээллийн илгээгч, агуулгын бүрэн бүтэн(засагдаагүй) байдлын баталгаа зэрэг төрөл бүрийн зорилгоор ашигладаг.

2.4 Тохиролцооны протоколууд

Өмнө хэлсэнчлэн, блокчэйн бол блок тус бүрийг нэг эгнээнд жагсаасан бүтэцтэй байдаг. Оролцох бүх зангилаа дээр ижил мэдээлэл бүхий блок ижил дарааллаар жагссан байх шаардлагатай. Уг блокийн дарааллыг шийдэх арга болгож блокчэйнд янз бүрийн нийцтэй байдлын алгоритмыг ашигладаг. Жишээлбэл, PoW(Proof of Work), PoS(Proof of Stake), PoI(Proof of Importance), PBFT(Practical Byzantine Fault Tolerance)

2.4.1 PoW(Proof of Work)

PoW бол bitcoinд ашиглагддаг алгоритм бөгөөд ерөнхийдөө майнинг/mining/ гэж нэрлэгддэг үйл ажиллагаанд хийгддэг зүйл юм. PoW-оор блок дотор агуулагддаг гүйлгээний мэдээлэл болон өмнөх блокийн хаш утган дээр санамсаргүй тоо(nonce) нэмж, хаш

утга тооцоолоод явна. Бодож олсон хаш утга урьдчилан тохируулсан шалгуур утгаас бага болтол нь санамсаргүй тоог өөрчилж, дахин тооцоолол хийнэ. Нөхцөлд таарах хаш утгыг олбол, уг блокийг идэвхтэй блок болгож, оролцогчдод түгээж, хүлээн зөвшөөрүүлнэ.

Хүлээн зөвшөөрөх тал нь хүрч ирсэн блоконд агуулагдах санамсаргүй тоо болон мэдээлэл тус бүрийн хаш утгыг зөвхөн нэг удаа тооцоолж үнэхээр блокчэйний нөхцөлийг хангаж байгаа эсэхийг шалгана. Энэ үед хийгдэх шалгах(тооцоолох) процесс нь зөвхөн нэг удаа хийгдэх бөгөөд майнинг хийхэд явагддаг их хэмжээний тооцоололтой харьцуулахад маш богино хугацаанд тооцон шалгаж болдог гэдгээрээ онцлогтой.

Bitcoin-д урьдчилан тохируулсан нөхцөлд таарсан блокийг үүсгэж чадсан нөхцөлд, блок үүсгэгчид урамшуулал болгон BTC/bitcoin/-г өгдөг.

Одоогийн байдлаар 1 блок үүсгэлтээр олж авах урамшуулал 12.5 BTC учраас хувь хүнд ногдох урамшуулал гэдэг утгаараа маш өндөр мөнгөн дүн юм. Bitcoin-д энэ мэтийн урамшууллаар мотивацилагдаж, хаш тооцооллын өрсөлдөөн явагдаж байдаг.

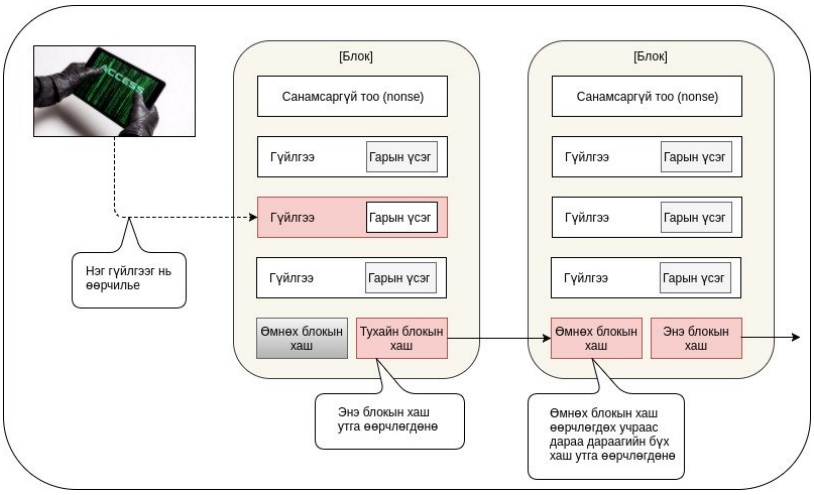
Нэмж хэлэхэд, bitcoin-ы майнингид Sha256 гэдэг алгоритм ашиглагддаг бөгөөд энэ алгоритмд зориулан оптимизаци хийгдсэн ASIC(Application Specific Integrated Circuit) гэдэг зориулалтын цахилгаан хэлхээ ашигласнаар өндөр хурдны майнинг хийх боломжтой болдог. Хаш утгын бодолтыг илэрхийлэх үзүүлэлт болгож хашрэйт(хаш үүсгэсэн тоо/секунд) ашиглагддаг бөгөөд 2017 оны 3 сарын байдлаар bitcoin систем бүхэлд нь авч үзвэл хашрэйт 3,252PH/s(Petahash/second) байдаг бөгөөд маш өндөр тооцон бодох чадвартай болохыг харж болно.

Харьцуулалт болгож, Intel Core i7 5820K бүхий CPU-гээр майнинг хийсэн тохиолдолд хашрэйт нь ойролцоогоор 10MH/s учир, хувь хүн CPU-гээр майнинг хийсэн нөхцөлд блок үүсгэх магадлал 325 тэрбумд 1 болох юм.Солир таарах магадлал 10 тэрбумын нэг гэж нэрлэгддэг учраас бодит байдал дээр CPU-гээр хожихгүй гэдэг нь тодорхой.

Bitcoin-д блокийг зэрэг олох магадлал байж болох учир олон газарт зэрэг олдсон тохиолдолд гинж салалт үүсэх болно. Ийм тохиолдолд, “Хамгийн урт гинж бүхий салаа нь хамгийн их хэмжээний тооцооллын зардлаар олдсон” гэдэг зарчим дээр тулгуурлаж, хамгийн урт гинж бүхий салааг сонгож авна гэсэн байдлаар явагдана. Хамгийн урт гинжийг сонгож авах арга нь гинжийг өөрчлөх асуудлын хувьд ч хамгаалалт болох үр нөлөөтэй.

Жишээ нь, хорон санаалсан хэрэглэгч, нэг блок дахь гүйлгээний агуулгыг өөрчилье

гэж үзсэн тохиолдлыг бодож үзье(Гүйлгээний мэдээллийг зассан үед).



Зураг 2.12: Гүйлгээний мэдээллийг зассан үед

Энэ тохиолдолд, гүйлгээний агуулгыг өөрчлөх учраас блокийн хаш утга бас өөрчлөгдөнө. Блокийн хаш утга өөрчлөгдмөгц, өмнө нь хангаж байсан нөхцөл (хаш утга шалгуур утгаас бага)-ийг хангаж чадахгүй болох учраас дахин санамсаргүй тоог өөрчилж, таарах хаш утгыг олох шаардлага үүснэ.

Энэ блок нь гинжний толгой хэсгээс /гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ бусад тохиолдолд, дараагийн блокод энэ блокийн хаш утга ашиглагдаж байгаа учраас, дараагийн блокийн хаш утгыг мөн өөрчилж бичих шаардлага үүснэ. Ингэмэгц, ээлж дараалан хаш утгыг дахин тооцоолж, хаш утгуудыг өөрчилж бичих шаардлага үүсч, энэ нь гинжний толгой/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэл үргэлжлэх хэрэгтэй болно. Засъя гэж бодсон блокоос блокийн эхэн/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэлх өөрчлөх хурд(өөрчлөгчийн тооцон бодох resource) нь жинхэнэ гинжний өсөх хурд (bitcoin системийн бүх тооцон бодох resource)-г давж гараагүй тохиолдолд уг дайралт амжилтгүй болох учраас гинжний өөрчлөлтийн эсрэг бат бөх гэж нэрлэгддэг.

Bitcoin-д хамгийн урт гинжийг хамгийн их зардал гаргасан гэж үздэг PoW(Proof of Work)-ийн тусламжтайгаар зангилаа хоорондын мэдээллийг нэгэн ижил саналд нийцүүлж байгааг танилцуулсан боловч, хувийн блокчэйнд оролцогч зангилааны тоог хязгаарлах боломжтой учраас, Paxos гэх мэт уламжлалт, түгээмэл тохиролцооны алгорит-

мыг ашиглах нь элбэг байдаг.

Нийтийн(public) болон хувийн (private) блокчэйний тохиролцооны алгоритмуудыг харьцуулбал, public блокчэйний сонгож авсан тохиролцооны алгоритм нь оролцогч зангилаануудын тоо олшрох тусам, гүйлгээний баталгаажуулалтын хурданд нөлөө гарах нь багасах шинж чанартай боловч, гүйлгээний процессын throughput/хурд/ өндөр биш юм.

Харин хувийн блокчэйнд зангилаа тоо нэмэгдэхэд гүйлгээний баталгаажуулалтын хурд буурах боловч, тогтсон тооны зангилаануудын хүрээнд өндөр throughput-тэй байж чаддаг.

2.4.2 Эцэслэн шийдэх чанар(finalty)

Нийтийн болон хувийн блокчэйний тохиролцооны алгоритмд finalty гэж нэрлэгддэг шинж чанарын ялгаа бас бий. Finalty гэдэг нь нэг удаа хийгдсэн гүйлгээний үр дүнг цуцлахгүй(эцэслэн шийдэх) гэдгийг илэрхийлнэ. Энэ чанар нь бодит байдал дээр гүйлгээ хийх үед чухал элемент гэж хэлж болно. Оролцох зангилаа-д хязгаарлалт байхгүй нийтийн блокчэйний хувьд finalty-г авч явах нь хэцүү юм.

Жишээ нь блокчэйн дээр Батын үлдэгдэл 1000 төгрөг гэж бичигдсэн байсан гэж үзье. “Батаас Дорж уруу илгээх 600 төгрөг(шилжүүлэг БД гэе)” болон “Батаас Болд руу илгээх 700 төгрөг(шилжүүлэг ББ гэе)” нь нэгэн зэрэг өөр өөр зангилаа уруу хүсэлт(request) явсан гэж үзье

Хараахан аль ч гүйлгээ нь блокчэйн дээр тэмдэглэгдээгүй учраас хүсэлт хүлээж авсан зангилаа-ууд аль ч гүйлгээнд Батад хангалттай үлдэгдэл байгаад, гүйлгээг хийхэд асуудалгүй гэж үзнэ. 2 гүйлгээ нь 2-уулаа хүлээн зөвшөөрөгдчихвөл Батын үлдэгдэл хасах 300 төгрөг болж, систем бүхэлдээ хасах үлдэгдэл гэсэн буруу байдалд шилжчихнэ.

Энэ асуудлыг шийдэхийн тулд, [Гүйлгээ БД] юм уу[Гүйлгээ ББ]-гийн аль нь “түрүүлж үүссэн” бэ гэдгийг шийдэх шаардлага гарч байна. [Гүйлгээ БД] нь [Гүйлгээ ББ]-гээс түрүүлж үүссэн гэж үзвэл, [Гүйлгээ БД]-гийн дуусах мөчид Батын үлдэгдэл 400 төгрөг болж, [Гүйлгээ ББ] нь үлдэгдэл мөнгө хүрэлцэхгүй учраас буруу шилжүүлэг болж, блокчэйнд бүртгэгдэхгүй. Эсрэгээрээ [Гүйлгээ ББ] нь [Гүйлгээ БД]-ээс түрүүлж үүссэн бол, [Гүйлгээ БД] нь буруу шилжүүлэг болно.

Нийтийн блокчэйнд зангилаа бүр өөрийн хадгалж буй статус дээр үндэслэж, гүйл-

гээний шалгалтыг явуулдаг. Гүйлгээний шалгалт дууссан үед шалгалт дууссаныг сүлжээн доторх зангилаа-уудад цацдаг(broadcast). Шалгалт дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалт зөв эсэхийг баталгаажуулаад өөрийн статусыг шинэчилдэг. Энэ зангилаа нь шинэ гүйлгээ шалгахаар бол, энэхүү шинэчлэгдсэн статус дээр үндэслэж гүйлгээг шалгана.

Дээр бичсэнчлэн, өөр өөр зангилаа дээр ялгаатай гүйлгээ бүр шалгагдаж, дууссан тухай мэдэгдэл сүлжээнд цацагдсан тохиолдолд, дууссан тухай мэдэгдлийг хүлээж авсан зангилаа өөрийн статусыг аль нэг гүйлгээний үр дүнгээр шинэчлэх шаардлага гарна. Энэ үед дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалтын үр дүн тус бүрийн гинжний аль уртыг нь сонгож, статусаа шинэчилнэ.

Гинжний уртаас хамаарч, өмнө нь орсон гүйлгээ нь блокчэйнд бичигдэнэ. Хойно нь орсон гүйлгээний хувьд, зангилаа нь өмнө орсон гүйлгээний үр дүнг тооцсоны дараах шинэчлэгдсэн статусаар дахин шалгалт явуулна.

Дахин шалгалтын үр дүнд, гүйлгээ нь үнэн зөв байвал сүлжээн дотор дахин цацаж(broadcast) бусад зангилаа дээр хүлээж авах хүртэл хүлээнэ. Харин буруу байвал, уг гүйлгээний хүсэлт нь алдаа болно.

Өмнөх жишээн дээр, [Гүйлгээ БД]-ийн гинж [Гүйлгээ ББ]-ийн гинжнээс урт бөгөөд, [Гүйлгээ БД] нь блокчэйнд бичигдсэн гэж үзье. Үүний үр дүнд, Батын хамгийн сүүлийн үлдэгдэл 1000 төгрөгөөс 600 төгрөгөөр хасагдаж, 400 төгрөг болно. Энэ байдалд, [Гүйлгээ ББ]-г шалгаад, үлдэгдэл хүрэлцэхгүй учраас [Гүйлгээ ББ] нь буруу гүйлгээ болж алдаа болно. [Гүйлгээ БД]-г шалгасан нөхцөлийг бодож үзвэл, үлдэгдэл 1000 төгрөг байх үед шалгаад зөв гэсэн дүгнэлт хийгээд, гүйлгээг гүйцэтгэсэн(сүлжээн доторх цацсан) боловч, түүний дараагаар өөр гүйлгээ гүйцэтгэгдэж, тэр нь давуу эрхтэй байсан учраас, үлдэгдэл нь 400 төгрөг болж, [Гүйлгээ БД] нь буруу болсон байна.

Нэгэн зэрэг хийгдэх гүйлгээ нь 2-оос олонгүй байна гэж мэдэж байгаа тохиолдолд, нэг талынх нь гүйлгээг дууссаны дараа нөгөө нэгийг нь гүйцэтгэвэл, дээрх шиг цуцлах тохиолдлыг гаргахгүй байж чадна. Гэвч, тодорхойгүй олон тооны зангилаа оролцож байгаа нийтийн блокчэйнд, нэгэн зэрэг хийгдэх гүйлгээ хэд байхыг хэлж мэдэхгүй. [Гүйлгээ БД] болон [Гүйлгээ ББ]-гээс өөр гүйлгээ бас нэгэн зэрэг хийгдэж байгаад, хоёр гүйлгээ хоёулаа цуцлагдах магадлал ч бий.

Энэ мэтчилэн нийтийн блокчэйнд гүйлгээг гүйцэтгэсэн үр дүн цуцлагдахгүй гэсэн finalty гэдэг шинж чанарыг хадгалж чаддаггүй.

Харин, оролцогч зангилаа-ын тоо нь хязгаарлагдсан хувийн блокчэйнд Paxos гэх мэтийн тохиролцооны алгоритмаар гүйлгээг эцэслэж чаддаг.

Жишээ нь, бүх зангилаа-оор олонхийн саналаар [Гүйлгээ БД]-г сонгох уу эсвэл [Гүйлгээ ББ]-г сонгох уу гэдгийг шийдэж чаддаг. Сонгогдсон гүйлгээ нь гинжин дээр бүртгэгдэж, түүнээс хойш цуцлагдахгүй болно. Олонхийн саналаар шийдэж байгаа болон үр дүнг нь бүх зангилаа дээр хүргэж чадаж байгаа нь оролцогч талуудын тоог хязгаарласан учраас юм.

2.4.3 Ухаалаг гэрээ(Smart contract)

Bitcoin-д зоос(койн)-ны шилжилтийн мэдээллийг бүх оролцогчдод дамжуулна гэсэн тогтолцоотой байсан. Үүний дээр, өөр мөнгөний мэдээлэл болон машин, үл хөдлөх хөрөнгийн эзэмших эрх гэх мэт зүйлсийг token/кодолсон тэмдэгтийн цуваа/ болгоод bitcoin-ы гүйлгээнд нэмэлт байдлаар оруулж, эдгээрийг өгч авалцдаг болгох өнгөт койн(colored coin) гэсэн санаа бас гарч ирсэн юм. Гэсэн хэдий ч, bitcoin-ы оршин байгаа тогтолцоог тэр хэвээр нь ашиглах учраас, агуулах мэдээллийн хэмжээнд хязгаар байгаа, мөн гүйлгээнд bitcoin хэрэгтэй болох зэрэг хязгаарлалтууд байсан. Иймд, Ethereum нь ухаалаг гэрээ гэдэг ойлголтыг оруулсан блокчэйн гэдгийг гаргаж, түүний дараагаар олон тооны блокчэйнд ухаалаг гэрээг оруулж ирсэн.

Ухаалаг гэрээг ашиглавал ямар зүйлийг хийж чаддаг болох вэ. Өргөн ашиглагддаг жишээ гэвэл “Автомат зарагч машинд зоос оруулахад, бараа гарч ирдэг” гэсэн дараалал бүхий урсгал бас ухаалаг гэрээ юм. Энэ мэтчилэн ямар нэг нөхцөлийн дор тогтсон үйлдэл хийдэг зүйлийг ухаалаг гэрээ гэж хэлдэг.

Ухаалаг гэрээ нь нэг үгээр хэлбэл “блокчэйн дээр ажиллана” гэсэн онцлогтой ердийн програм гэж хэлж болно. Ухаалаг гэрээ нь блокчэйн болгоноор нэршил нь өөр өөр байдаг боловч, цаанаа бодит бие нь Javascript(төрлийн хэл), Golang, Java, C# гэх мэтийн ердийн програмчлалын хэлээр бичиж болох програм бөгөөд блокчэйний статус болон хадгалагдаж байгаа дата зэргийг уншиж бичих зориулалттай зүйл юм.

Гэхдээ, “Блокчэйн дээр ажиллана” гэдэг дээр анхаарах зүйл бий. Энэ үгнээс ямар ажиллагаа төсөөлөгдөж байна вэ? Блокчэйн бүхэлдээ 1 нийтлэг процессын байгууллага, эсвэл оролцогчдын аль нэг нь төлөөлөөд програмыг ажиллуулдаг гэж төсөөлөгдөж байна уу. Үнэндээ аль алинаас нь өөр бөгөөд, бүх зангилаа дээр ижил програм ажиллаж, хариултыг нь тааруулдаг гэсэн ажиллагаа болж байгаа юм.

Блокчэйн дээр бүх зангилаа нь ижил дата хуваалцдаг, гэдгийг аль хэдийнээ тайлбарласан боловч, энэ нь ухаалаг гэрээний хувьд ч мөн нэгэн адил юм.

Ердийн програмд санамсаргүй тоо ашиглаж, гаднах өгөгдлийн эх сурвалжаас утга олж авчирч, процесс хийх зэргийг ихэвчлэн хийдэг боловч, энэ мэт тодорхой бус шинжийг агуулсан ажиллагаа нь нэгэн ижил өгөгдлийг хуваалцана гэсэн шинж чанарыг баримтлах шаардлагатай ухаалаг гэрээний хувьд чадахгүй зүйл бөгөөд детерминистик (тогтсон, тодорхой) байдлаар бүх процесс үргэлжилж байх шаардлагатай.

Ажиллуулах бүрд санамсаргүй тоо ашиглах эсвэл гадны сервертэй холбогдох шаардлагатай үед тэдгээр үйлдлүүдийг oracle гэж нэрлэгддэг 3-дагч этгээдээр гүйцэтгүүлж, олсон утгыг нь ухаалаг гэрээнд дамжуулах гэсэн арга бий. Энэ тохиолдолд, блокчэйн нь зорин байж хийсэн тархмал систем учраас oracle нь цорын ганц эвдрэлийн цэг болохооргүй байх хэрэгтэйг анхаарах хэрэгтэй.

Бүлэг 3

Судалгаа

Бүлэг 4

Төслийн хэсэг